UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Brian Walton,

Plaintiff,

v.

Medtronic USA, Inc.,

Defendant.

Case No. 22-cv-50 (PJS/JFD)

ORDER

This matter is before the Court on a disagreement between the parties, Medtronic USA, Inc. and Brian Walton, on the appropriate terms of a protocol for the discovery of electronically stored information ("ESI"). The Court heard arguments from both parties on December 5, 2022. (Hr'g Mins., Dkt. No. 54.) Defendant Medtronic was represented by Claire B. Deason, Daniel Bihrle, Katherine Tank, and Marco J. Mrkonich. (*Id.*) Plaintiff Mr. Walton was represented by Colin John Pasterski. (*Id.*) After reviewing the proposed stipulation of the parties submitted to the Court via email, and considering the arguments of counsel, the Court **ORDERS** the parties to comply with the following protocol for the discovery of ESI.

I. GENERAL TERMS

A. Legibility. The Parties will make reasonable efforts to ensure that all Documents and ESI they produce are legible. If a copy is not legible and it is possible to produce a legible copy, such a legible copy will be produced (subject to relevant general and specific objections) within five (5) business days of a request from a receiving Party, or as mutually agreed upon by the Parties. But if no legible copy can be made, then the original will be made available for inspection and copying within ten (10) business days of a request from a receiving Party, or as mutually agreed upon by the Parties.

B. Definition of Native File(s). The meaning of Native File(s) is ESI in the electronic format of the application in which such ESI is normally created, viewed, and/or modified.

II. SEARCH TERMS FOR ELECTRONIC DOCUMENTS

If there is a dispute over a discovery demand as to which a full response will require review of ESI, the meet and confer process as to that discovery demand will include the parties cooperating in good faith regarding the disclosure and formulation of appropriate search methodology, terms, and protocols in advance of any ESI search. With the objective of limiting the scope of review and production, and thereby reducing discovery burdens, the Parties will meet and confer as early as possible concerning any such discovery demand, and in advance of any producing party search commencement, to discuss, *inter alia*:

- Search methodology (Boolean, technology assisted review)
- Pre-search-commencement disclosure of all search terms, including semantic synonyms. Semantic synonyms shall mean without limitation code words, terms, phrases or illustrations, acronyms, abbreviations, or non-language alphanumeric associational references to relevant ESI, or information that may lead to relevant ESI.
- Search protocol (algorithm selection, etc.)
- Custodians.
- Post-search error sampling and sampling/testing reports.

The parties will continue to meet and confer regarding any search process issues as necessary and appropriate.

III. PRODUCTION OF DOCUMENTS

A. File Type. The Parties shall produce Documents as Group IV single-page TIFF images (for black-and-white content) and JPEG image files (for color content) at not less than

300 dpi resolution, along with associated document-level text files, image load files (.DII, LFP, and OPT) indicating appropriate document and family breaks, as well as metadata load files in delimited text format containing the fields required by Section III(B). The TIFF image must convey the same information as if the Document were produced in paper.

B. Extracted Text and OCR. For documents that do not contain redactions, the producing Party will produce an extracted text file for each electronic document where text can be extracted, and an Optical Character Recognition ("OCR") text file for (i) each imaged paper document, and (ii) each electronic document for which text cannot be extracted. For documents that contain redactions, the producing Party will provide an OCR text file for the unredacted portions of such documents. Said extracted text and OCR files shall be produced as document level text files and be named consistently with their corresponding TIFF files ([producing Party's Name]-000000001.tif and [producing Party's Name]-000000001.txt). The Parties shall confer to identify the list of file types for which text cannot be extracted, and for which OCR text will thus be provided by the producing Party at the time of production pursuant to this paragraph. The Parties recognize that agreeing to a specific list now is premature as the Parties first need to understand which file types might be relevant.

C. Family Groups. The Parties shall maintain family groups together in one production volume and shall not break family groups apart in separate production volumes.

D. Unitization. All productions will be unitized to ensure logical separation between e-mails, attachments, and other individual documents.

E. Scan Size. Reasonable efforts will be used to scan Documents at or near their original size, so that the print or image on the Document appears straight, and not skewed. Reducing image size may be necessary to display production numbers and confidentiality designations without obscuring text. Physically oversized originals will appear reduced. A producing Party reserves the right to determine whether to produce oversized Documents in their original size. A receiving Party may request that specific oversized Documents be produced in their original size for good cause.

F. Notes and Attachments. If any original Document has notes or attachments affixed thereto, the Parties will produce copies of those Documents with the accompanying notes and attachments unless privileged or exceptioned during processing.

IV. PRODUCTION OF ESI

A. File Type. The Parties shall produce ESI as Group IV black and white or color, single-page TIFF images at not less than 300 dpi resolution, along with associated document-level text files, image load files (.DII, LFP, and OPT) indicating appropriate document and family breaks, as well as metadata load files in delimited text format containing the fields required by Section III(B).

B. Metadata. For each item of ESI, if applicable, the Parties shall identify the following metadata:

Metadata List	
1	Production Beg Num
2	Production End Num
3	Production Beg Attach
4	Production End Attach
5	Custodian
6	Confidentiality Designation
7	MD5 Hash (digital fingerprint for authentication)
8	Message To
9	Message From
10	Message CC
11	Message BCC

12	Message Date Sent (Date-Time Sent)
13	Message Date Received (Date-Time Received)
14	Time Zone
15	Message Subject
16	File Name
17	File Extension
18	File Date Created (date and time created)
19	File Date Last Modified (date and time modified)
20	File Author
21	Record Type
22	Page Count
23	Native Link (file-path and file-name indicating where natively-produced exceptions – Excels and audio/video content – are located within the production)
24	Extracted-Text Link (file-path and file-name indicating where the extracted-text text file corresponding to each record is stored)

The Parties will take reasonable steps to preserve, to the extent they have a value, all Metadata associated with ESI even if such Metadata is not specified above for production.

C. Native Files. Microsoft PowerPoint and Excel files, as well as audio-visual content, shall be produced as Native Files unless redactions are required. Tiff images should also be produced for all PowerPoint or presentation files. For Excel and other spreadsheet files, the Parties will produce a single slipsheet for each Excel file branded with the text "File Produced In Native Format" along with the corresponding Bates number and confidentiality designation. A Party may request that another Party produce other ESI as Native Files for good cause.

D. Production Format for Databases and Audio-Visual Files. The Parties will meet and confer regarding the production format for Microsoft Access or other similar databases.

E. De-duplication. A party is only required to produce a single copy of a responsive document and shall deduplicate responsive ESI (based on MD5 or SHA-1 hash values) globally.

F. Attachments. If any original ESI has attachments, the Parties will produce copies of that ESI with the attachments unless privileged, not responsive to a discovery request, or exceptioned during processing.

G. Unitization. All productions will be unitized to ensure logical separation between e-mails, attachments, and other individual documents.

H. Archived Materials. Absent a showing by the requesting Party of circumstances whereby the need for such ESI substantially outweighs the burden associated with recovering it and that no other source for such ESI is otherwise available, the Parties shall not be required to search Back-Up Tapes and Data or other back-up, archived, or disaster recovery systems. For purposes of this Section, "Back-Up Tapes and Data" means data duplicated in any electronic backup system for the purpose of system recovery or information restoration, including but not limited to, system recovery backup tapes, continuity of operations systems, and data or system mirrors or shadows, if such data are routinely purged, overwritten or otherwise made not reasonably accessible in accordance with an established routine system maintenance policy.

I. Preservation Not Required for Not Reasonably Accessible ESI. The Parties need not preserve, search for, or produce (a) deleted computer files, whether fragmented or whole, (b) temporary or cache files, including internet history, web browser cache and cookie files, and (c) server, system, or network logs.

V. BATES LABELING/CONFIDENTIALITY DESIGNATIONS

A. Labeling. Each page of all images produced must be clearly labeled with an indelible, legible, unique Bates number identifier electronically "burned" onto the image. Reasonable steps shall be taken to place the Bates number at a location that does not obscure any information from the source document. In addition, to the extent any image or file is to be marked confidential, each page of the image or file to be marked confidential shall include the appropriate confidentiality designation as determined in the Protective Order separately entered into by the Parties. There shall be no other legend or stamp placed on the document image, with the exception of redacted information due to claims of applicable privileges.

B. Consecutive Numbering. The Parties agree that a convention on Bates number ordering will help the Parties better organize production of Documents and ESI in this Action. Therefore, to the extent possible, Documents and ESI shall be Bates-numbered consecutively by custodian (source), maintaining all parent-child relationships. Document numbers for documents produced by the Parties shall identify the Party's name and shall be in the format "Party Name- 00000001."

C. File Names. Image file names must be unique and must correspond with the Bates number imprinted on the image. For example, if the Bates number "B0000001" was imprinted, the image would bear the name "B0000001.tif."

D. Authenticity. The parties have agreed that they shall not object that Documents or ESI produced pursuant to this Stipulation are not authentic based upon the file naming convention described in Section IV(C), above. The Parties otherwise reserve all rights regarding their ability to object to the authenticity of Documents or ESI.

E. Native Files. If Native Files are produced, the Party producing such Native File shall include a single-image placeholder TIFF with a single Bates number on the image itself. As stated above, the slipsheet for each native Excel file will include the text "File Produced In Native Format" along with the corresponding Bates number and confidentiality designation. The Native File shall be renamed to match the Bates number assigned thereto. There shall be no Bates numbering of Native Files at the page level.

VI. INFORMATION SECURITY PROTECTIONS

A. Any person in possession of another party's confidential information shall maintain a written information security program that includes reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such confidential information, protect against any reasonably anticipated threats or hazards to the security of such confidential information, and protect against unauthorized access to or use of such confidential information. To the extent a person or party does not have an information security program they may comply with this provision by having the confidential information managed by and/or stored with eDiscovery vendors or claims administrators that maintain such an information security program.

If the Receiving Party discovers a breach of security, including any actual or suspected unauthorized access, relating to another party's confidential information, the Receiving Party shall: (1) promptly provide written notice to Designating Party of such breach; (2) investigate and take reasonable efforts to remediate the effects of the breach, and provide Designating Party with assurances reasonably satisfactory to Designating Party that such breach shall not recur; and (3) provide sufficient information about the breach that the Designating Party can reasonably ascertain the size and scope of the breach. If required by any judicial or governmental request, requirement or order to disclose such information, the Receiving Party shall take all reasonable steps to give the Designating Party sufficient prior notice in order to contest such request, requirement or order through legal means. The Receiving Party agrees to cooperate with the Designating Party or law enforcement in investigating any such security incident. In any event, the Receiving Party shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.

VII. PRIVILEGE AND REDACTIONS

A. Entire Categories of Privileged Documents. The Parties recognize that there may be a limited number of instances where there are categories or groups of Documents or ESI in which all items are privileged and that, because of the large number of individual items in such a category or group, it would be a great burden to separately identify on a privilege log each individual Document or item of ESI included in that group. The Parties agree that in such instances, in accordance with The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production, comment 3(c) (2007 ed.) and as appropriate, instead of separately identifying each Document or item of ESI on its privilege log, it may instead identify categories or groups of privileged Documents or privileged ESI. In so doing, the Party shall describe in its privilege log the category or group of privileged Documents or ESI (including, without limitation, the criteria and method of delimiting the category or group), the factual basis for a reasonable belief that all Documents or ESI in the category or group are privileged, and the legal basis for the assertion of a privilege as to all Documents or ESI in the category or group. Additionally, if a Party requests further information relating to a category or group identified on another Party's privilege log, such information shall be provided so that the requesting Party has sufficient information to determine whether or not to challenge the privilege claim. The ultimate adjudication of challenged privilege claims shall be made on the basis of a document-by-document review. The parties agree that documents directed to or created by outside counsel on or after January 10, 2022, the date the Complaint was filed, need not be identified on privilege logs, without any waiver of privilege or work product protection for such documents.

B. Redactions. If the producing Party is redacting information from a page, the producing Party shall electronically "burn" the word "Redacted" onto the page at or reasonably near to the location of the redaction(s). If the producing Party redacts a document, the following metadata fields must nonetheless be produced to the extent the fields are already populated in the ordinary course:

Field Name	**Description**
ProdBeg	Beginning bates number
ProdEnd	Ending bates number
ProdBegAttach	Beginning attachment number
ProdEndAttach	Ending attachment number
FileExt	Efile field - DocType (the file name suffix of an electronic file)
Sent Date	Email field – Sent Date
Last Modified Data	Efile Field – Modification Date
Create Date	Efile field – Creation Date
Custodian (s)	Global deduplication was performed so multiple custodians will be supplied in this field.

C. Clawback. The inadvertent disclosure to another Party of any document which is subject to a legitimate claim that the document should have been withheld from disclosure as a privileged attorney/client communication or attorney work product shall not constitute a waiver of any privilege or otherwise affect the right to withhold it from production as privileged or work product.

If, during the course of this litigation, any party determines that any document produced by another party is or may reasonably be subject to a legally recognizable privilege or evidentiary protection ("Protected Document"), the Receiving Party shall: (1) refrain from reading the Protected Document any more closely than is necessary to ascertain that it is privileged or otherwise protected from disclosure; (2) immediately notify the Producing Party in writing that it has discovered Documents believed to be privileged or protected; (3)

specifically identify the Protected Documents by Bates number range or hash value, and, (4) within ten (10) days of discovery by the Receiving Party, return, sequester, or destroy all copies of such Protected Documents, along with any notes, abstracts or compilations of the content thereof. To the extent that a Protected Document has been loaded into a litigation review database under the control of the Receiving Party, the Receiving Party shall have all electronic copies of the Protected Document extracted from the database. Where such Protected Documents cannot be destroyed or separated, they shall not be reviewed, disclosed, or otherwise used by the Receiving Party. Notwithstanding, the Receiving Party is under no obligation to search or review the Producing Party's Documents to identify potentially privileged or work product Protected Documents.

If, in the alternative, a request is made in good faith to return any such allegedly privileged or work product document that was inadvertently disclosed, the Party that received the document shall delete it and return all hard copies of it within 10 days of the request. The privilege or work product status of such document or information, if any, shall be deemed to be restored upon the making of such request, provided, however:

(1) Nothing herein shall preclude the non-producing party from requesting the Court to determine whether the document or information is privileged or work product. In the event the non-producing party intends to challenge the claim of privilege or work product, the non-producing party may retain a copy of such document for such purposes.

(2) If the producing party either (i) expresses the intent to use such document or information at a hearing, deposition, or trial, or (ii) uses such document or information at a hearing, deposition, or trial, the producing party's right to request a return of such

document or information shall be foreclosed. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).

Date: December 5, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge